Active information gathering

Once the passive phase is over it is time to move to the active phase. In this phase we start interacting with the target.

Netdiscover

This tool is used to scan a network for live machines.

```
netdiscover -r 192.168.1.1/24
```

Nikto

Nikto is a good tool to scan webservers. It is very intrusive.

```
nikto -host 192.168.1.101
```

References

https://blog.bugcrowd.com/discovering-subdomains

https://high54security.blogspot.cl/2016/01/recon-ng-and-power-to-crawl-trough.html